RECEIVED
CENTRAL FAX CENTER

JUN 06 2006

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

ATTY. DOCKET NO.: RPS920010156US1

IN RE APPLICATION OF:	§	
DARYL CARVIS CROMER ET AL.	§	EXAMINER: **VENKATANARAY PERUNGAVOOR**
SERIAL NO.: **10/077,135**	§	
FILED: **FEBRUARY 15, 2002**	§	ART UNIT: **2132**
FOR: **METHOD AND SYSTEM FOR SECURING ENABLEMENT ACCESS TO A DATA SECURITY DEVICE**	§	

APPEAL BRIEF UNDER 37 C.F.R. 1.192

Mail Stop Appeal Briefs - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

Sir:

This Appeal Brief is submitted in support of an Appeal of the Examiner's final rejection of claims 1-3, 5-12, 14-21, and 23-26. A Notice of Appeal in this case was filed and received by the patent office on April 18, 2006. Please charge the fee of $500.00 due under 37 C.F.R. § 1.17(c), as well as any additional required fees, to IBM Deposit Account No. 09-0447. 1402

Certificate of Transmission/Mailing

I hereby certify that this correspondence is being facsimile transmitted to the USPTO at 571-273-8300 or deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450 on the date shown below.

Typed or Printed Name: Michelle Sanderson *Date:* June 6, 2006 *Signature:* /Michelle Sanderson/

06/07/2006 CNGUYEN2 00000055 090447 10077135

01 FC:1402 500.00 DA

RECEIVED
CENTRAL FAX CENTER

JUN 06 2006

REAL PARTY IN INTEREST

The real party in interest in the present Application is International Business Machines Corporation, the Assignee of the present application as evidenced by the Assignment set forth at reel 012620, frame 0620 et. seq. of the USPTO assignment records.

RELATED APPEALS AND INTERFERENCES

There are no other appeals or interferences known to Appellants, the Appellants' legal representative, or assignee, which directly affect or would be directly affected by or have a bearing on the Board's decision in the pending appeal.

STATUS OF CLAIMS

Claims 1-3, 5-12, 14-21, and 23-26 stand finally rejected by the Examiner, as noted in the final Office Action dated March 18, 2006. The rejection of Claims 1-3, 5-12, 14-21, and 23-26 is appealed.

STATUS OF AMENDMENTS

Appellants' Amendment A filed on December 16, 2005 was entered by the Examiner as indicated in the final Office Action. No amendment to the claims was proposed or entered subsequent to the Amendment A filed on December 16, 2005.

SUMMARY OF THE CLAIMED SUBJECT MATTER

Appellant's invention may be implemented as a method, apparatus, or a computer program product for controlling access to a data security device within a data processing system. As explained in Appellants' specification (see page 2, line 4, *et seq.*; page 7, line 22 through page 8, line 3; page 9, lines 22-26), hardware security devices such as the data access enablement/disablement mechanisms (e.g. security bit settings) employed by embedded security subsystems are vulnerable to security breaches when they are initially set in the absence of user authorization coinciding with the startup procedure. Appellants' proposed invention fortifies secure access to setting the enablement/disablement mechanism, which may comprise one or more security bits, by utilizing a "pending state change flag" and a "persistent enable flag" that

cooperatively ensure that the access enablement mechanism (in part comprising the persistent enable flag itself) may only be set or reset in connection with a system power-on reset event.

Specifically, Appellant's claim 1 recites an apparatus for "for controlling access to a data security device within a data processing system" comprising "a persistent enable flag for providing control access to said data security device, wherein said persistent enable flag is write-accessible only in response to a detected power-on reset of said data processing system," (*see specification* page 10, line 25 through page 11, line 5; page 11, lines 13-22; page 12, lines 7-22; page 16, lines 8-12, generally describing with reference to **FIG. 2** a Trusted Platform Management (TPM) enable flag **45** utilized for determining the enabled/disabled status of a TPM module **32**; see page 11, lines 16-22, contrasting conventional techniques (i.e. prior art) by which TPM enable flags may be set/reset with the power-on reset mechanism utilized by invention; *see specification* page 4, lines 13-16, describing setting persistent enable flag responsive to detecting re-application of system power; page 12, lines 10-19, describing power-on reset gating mechanism for setting TPM enable bit **45**; page 13, lines 11-21, describing boot reset process as an exclusive condition for changing enablement status of TPM enable flag **45**; see page 14 lines 8-20, describing a power-on reset state detection latch **48** read by processing unit **40** to determine whether to read a pending state flag bit **41** and setting TPM enable flag bit **45** accordingly; see page 18, claim 1, lines 4-5).

Claim 1 continues "and wherein said persistent enable flag is read-only accessible to runtime program instructions" (*see specification* page 4, line 8; page 12, lines 19-22; page 19, claim 4, lines 2-3; page 21, claim 13, lines 2-3; page 23, claim 22, lines 2-3; Abstract).

The invention as recited in claim 1 provides a mechanism in the form of a "pending state change flag bit" in conjunction with power-on reset procedures for securing the conditions under which the claimed "persistent enable flag" may be set/reset. To this end, the apparatus recited in claim 1 further includes "a pending state change flag write-accessible by runtime program instructions, for setting an intended next state of said persistent enable flag such that control access to said data security device is enabled only during a subsequent power-on reset of said data processing system." *See specification* page 12, lines 10-19 and page 13, lines 10-21 (generally describing with reference to **FIG. 2** utilization of a setting of pending state flag **41** in concert with a power-on reset to determine the setting of persistent enable flag 45); page 12, line

23 through page 13, line 21 (describing input devices such as a user keyboard that may be used "during runtime operations" to access pending state flag **41**); page 16, lines 14-17 (explaining with reference to **FIG. 3** that pending state change flag is write accessible during runtime program instruction operations); page 14, lines 4-20 (explaining, with reference to **FIG. 2**, that the reading of pending state flag **41** and consequent setting of persistent enable bit **45** occurs exclusively in connection with a power-on reset cycle).

The invention recited in independent claim 9 is a method "for providing secure controllability of a data security device within a data processing system" comprising "responsive to detecting a power-on reset cycle initiated within said data processing system:

determining the state of a pending state change flag" (*see specification*, page 14, lines 4-20 (explaining, with reference to **FIG. 2**, that the reading of pending state flag **41** and consequent setting of persistent enable bit **45** occurs exclusively in connection with a power-on reset cycle), "wherein said pending state change flag is write-accessible by runtime program instructions for setting an intended next state of a persistent enable flag that enables or disables runtime control access to said data security device," (*see specification*, page 12, line 23 through page 13, line 21 (describing input devices such as a user keyboard that may be used "during runtime operations" to access pending state flag **41**); page 16, lines 14-17 (explaining with reference to **FIG. 3** that pending state change flag is write accessible during runtime program instruction operations; page 12, lines 10-19 and page 13, lines 10-21 (generally describing with reference to **FIG. 2** utilization of a setting of pending state flag **41** in concert with a power-on reset to determine the setting of persistent enable flag **45**)) "wherein said persistent enable flag is read-only accessible to runtime program instructions" (*see specification* page 4, line 8; page 12, lines 19-22; page 19, claim 4, lines 2-3; page 21, claim 13, lines 2-3; page 23, claim 22, lines 2-3; Abstract).

In further response to the detected power-on reset cycle, claim 9 recites a step of "setting or resetting said persistent enable flag in accordance with the state of said pending state change flag." *See specification*, page 10, line 25 through page 11, line 5; page 11, lines 13-22; page 12, lines 7-22; page 16, lines 8-12, generally describing with reference to **FIG. 2** a Trusted Platform Management (TPM) enable flag **45** utilized for determining the enabled/disabled status of a TPM module **32**; see page 11, lines 16-22, contrasting conventional techniques (i.e. prior art) by which TPM enable flags may be set/reset with the power-on reset mechanism utilized by invention; page 4, lines 13-16, describing setting persistent enable flag responsive to detecting re-

application of system power; page 12, lines 10-19, describing power-on reset gating mechanism for setting TPM enable bit **45**; page 13, lines 11-21, describing boot reset process as an exclusive condition for changing enablement status of TPM enable flag **45**; see page 14 lines 8-20, describing a power-on reset state detection latch **48** read by processing unit **40** to determine whether to read a pending state flag bit **41** and setting TPM enable flag bit **45** accordingly; see page 18, claim 1, lines 4-5.

The invention recited in independent claim 18 is a computer-readable medium having encoded thereon computer-executable instructions "for providing secure controllability of a data security device within a data processing system" having computer-executable instructions adapted for executing a method comprising "*program instructions* responsive to detecting a power-on reset cycle initiated within said data processing system *for*:"(note "program instructions" and "for" removed in attached amendment of claim 18)

"determining the state of a pending state change flag" (*see specification,* page 14, lines 4-20 (explaining, with reference to **FIG. 2**, that the reading of pending state flag **41** and consequent setting of persistent enable bit **45** occurs exclusively in connection with a power-on reset cycle), "wherein said pending state change flag is write-accessible by runtime program instructions for setting an intended next state of a persistent enable flag that enables or disables runtime control access to said data security device," (*see specification*, page 12, line 23 through page 13, line 21 (describing input devices such as a user keyboard that may be used "during runtime operations" to access pending state flag **41**); page 16, lines 14-17 (explaining with reference to **FIG. 3** that pending state change flag is write accessible during runtime program instruction operations; page 12, lines 10-19 and page 13, lines 10-21 (generally describing with reference to **FIG. 2** utilization of a setting of pending state flag **41** in concert with a power-on reset to determine the setting of persistent enable flag **45**)) "wherein said persistent enable flag is read-only accessible to runtime program instructions" (*see specification* page 4, line 8; page 12, lines 19-22; page 19, claim 4, lines 2-3; page 21, claim 13, lines 2-3; page 23, claim 22, lines 2-3; Abstract).

In further response to the detected power-on reset cycle, claim 18 recites "setting or resetting said persistent enable flag in accordance with the state of said pending state change flag." *See specification*, page 10, line 25 through page 11, line 5; page 11, lines 13-22; page 12, lines 7-22; page 16, lines 8-12, generally describing with reference to **FIG. 2** a Trusted Platform Management (TPM) enable flag **45** utilized for determining the enabled/disabled status of a TPM

module **32**; see page 11, lines 16-22, contrasting conventional techniques (i.e. prior art) by which TPM enable flags may be set/reset with the power-on reset mechanism utilized by invention; page 4, lines 13-16, describing setting persistent enable flag responsive to detecting re-application of system power; page 12, lines 10-19, describing power-on reset gating mechanism for setting TPM enable bit **45**; page 13, lines 11-21, describing boot reset process as an exclusive condition for changing enablement status of TPM enable flag **45**; see page 14 lines 8-20, describing a power-on reset state detection latch **48** read by processing unit **40** to determine whether to read a pending state flag bit **41** and setting TPM enable flag bit **45** accordingly; see page 18, claim 1, lines 4-5.

GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

The rejection of claims 1-3, 5-12, 14-21, and 23-26 under 35 U.S.C. §102(b) as being anticipated by U.S. Pat. No. 5,826,007, issued to *Sakaki et al.* (hereinafter *Sakaki*) is to be reviewed on Appeal.

ARGUMENT

A. The rejection of claims 1, 9, and 18 under 35 U.S.C. §103(a) as being anticipated by *Sakaki* is not well founded and should be reversed.

1. *Sakaki* does not disclose an apparatus that includes each claimed feature of claim 1

Regarding independent claim 1, *Sakaki* fails to disclose or suggest an apparatus for controlling access to a data security device within a data processing system that includes "a persistent enable flag for providing control access to said data security device, wherein said persistent enable flag is write-accessible only in response to a detected power-on reset of said data processing system, and wherein said persistent enable flag is read-only accessible to runtime program instructions." The final Office Action asserts on page 3, reference item 8, that *Sakaki* discloses a persistent enable flag that is write-accessible only in response to a detected power-on reset (col. 3, lines 21-40 and col. 4, lines 49-56, Fig. 1, bit S2; col. 5, line 34 – col. 6, line 7), wherein the persistent enable flag is read-only accessible to runtime program instructions (col. 4, lines 43-56). With reference Sakaki's Fig. 2, the foregoing passages describe a two bit security flag comprising S1 and S2. A security flag monitor circuit 25 reads the single security flag comprising S1 and S2 in response to a power-on reset. Nowhere does *Sakaki* specify that the S2 flag (or S1) performs a persistent enablement function in a manner in which the *write*-accessibility of S2 (or S1) is in any way affected by whether or not a power-on reset has been detected. In fact, at col. 4, lines 50-54 describes application of a control input /CE and a write input /WR as the conditions under which a write is performed on the two-bit flag with no mention of a power-on reset as a necessary condition.

In further regarding to claim 1, *Sakaki* fails to disclose or suggest "a pending state change flag write-accessible by runtime program instructions, for setting an intended next state of said persistent enable flag such that control access to said data security device is enabled only during a subsequent power-on reset of said data processing system." Notably, in neither the first Office

Action, dated August 16, 2005, nor the final Office Action, nor the Advisory Action dated April 17, 2006 does the Examiner assert that *Sakaki* discloses the foregoing element. Instead, and presumably relating to the foregoing "pending state change flag" limitation, the final Office Action asserts on page 3, reference item 8, that *Sakaki* discloses an enable flag (Fig. 2, bit S1) being used to control access to a device (memory devices 12 and 17 in Figs. 1 and 2; col. 5, lines 24-33). Nowhere does *Sakaki* disclose (nor does the Examiner assert) that the S1 flag (or S2) sets an intended next state of the other, S2 (or S1), "persistent enable flag."

Appellants contend that the S1 and S2 bits disclosed by *Sakaki* do not share the functional characteristics of the "persistent enable flag" and "pending state change flag" recited in Appellants' claim 1. The S1 and S2 bits disclosed by *Sakaki* constitute a single security flag that is monitored by a security flag monitor circuit 25 which reads the two-bit flag when receiving a power-on reset signal and provides a recognition result to a bus line control circuit (see col. 4, lines 42-61, and col. 5, lines 15-33). Nothing in the description of the two-bit security flag consisting of bits S1 and S2 or elsewhere does *Sakaki* disclose the equivalent of a persistent enable flag that is "write-accessible only in response to a detected power-on reset" and is "read-only accessible to runtime program instructions" as required by the express claim body language of Appellants' claim 1. Furthermore, *Sakaki* does not disclose a system including the foregoing persistent enable flag that further includes a pending state change flag for setting an intended next state of the persistent enable flag and that, unlike the persistent enable flag, is write-accessible by runtime program instructions. In fact, *Sakaki* includes no disclosure or suggestion that the flag bits S1 and S2 are functionally distinct in terms of protection/accessibility (i.e. write-only accessible versus read-only accessible to runtime program instruction; write-accessible only in response to a detected power-on reset).

2. *Sakaki* does not disclose each claimed feature of claims 9 and 18

Regarding the grounds for rejecting independent claims 9 and 18, the Final Office Action asserts in reference item 13 on pages 4-5, that *Sakaki* substantially discloses the setting/resetting of persistent and pending flags executed through runtime instructions (col. 5, lines 21-30; col. 4, lines 58-65; and col. 5, lines 43-47). At col. 4, lines 58-61, *Sakaki* discloses the general concept of reading a security flag coincident with receiving a power-on reset signal. However, neither in the foregoing passages nor elsewhere does *Sakaki* disclose or suggest a step of, in response to a power-on reset cycle, determining the state of a pending state change flag that is write-accessible

by runtime programs to set an intended next state of a persistent enable flag that enables or disables access to the device and setting or resetting the persistent enable flag in accordance with the state of the pending state flag.

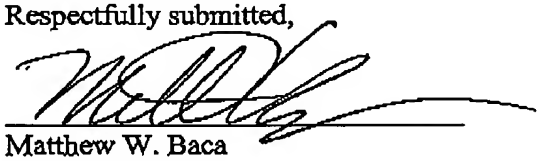
B. The rejection of claims 2-3, 5-8, 10-12, 14-17, 19-21, and 23-26 under 35 U.S.C. §102(b) as being anticipated by *Sakaki* is not well founded and should be reversed.

Appellants do not concede that *Sakaki* actually teaches or suggests any of the features of these dependent claims; however, these claims are directly or indirectly dependent on the independent claims 1, 9, and 18 which, as contended above by Appellants, have been incorrectly rejected under the references. By extension, the rejections of claims 2-3, 5-8, 10-12, 14-17, 19-21, and 23-26 are not well founded and should be reversed.

CONCLUSION

Appellants have pointed out with specificity the manifest error in the Examiner's rejections, and the claim language that renders the invention patentable over *Sakaki*. Appellants, therefore, respectfully requests that this case be remanded to the Examiner with instructions withdraw the present claim rejections.

Respectfully submitted,



Matthew W. Baca
Reg. No. 42,277
DILLON & YUDELL LLP
8911 N. Capital of Texas Highway
Suite 2110
Austin, Texas 78759
512-343-6116

ATTORNEY FOR APPELLANTS

CLAIMS APPENDIX

1. An apparatus for controlling access to a data security device within a data processing system, said apparatus comprising:

a persistent enable flag for providing control access to said data security device, wherein said persistent enable flag is write-accessible only in response to a detected power-on reset of said data processing system, and wherein said persistent enable flag is read-only accessible to runtime program instructions; and

a pending state change flag write-accessible by runtime program instructions, for setting an intended next state of said persistent enable flag such that control access to said data security device is enabled only during a subsequent power-on reset of said data processing system.

2. The apparatus of claim 1, further comprising:

a switched power input to said data security device;

a power-on reset detection latch for detecting the occurrence of power applied by said switched power input; and

means for determining the state of said power-on reset detection latch.

3. The apparatus of claim 2, further comprising means responsive to determining a set state of said power-on reset detection latch for:

determining the state of said pending state change flag; and

determining a next state of said persistent enable flag in accordance with the determined state of said pending state change flag.

4. (Cancelled)

5. The apparatus of claim 1, wherein said persistent enable flag and said pending state change flag are non-volatile storage devices.

6. The apparatus of claim 1, wherein said data security device includes memory for receiving and storing data.

7. The apparatus of claim 1, wherein said data security device includes security portal functionality for controlling access to data stored within said data processing system.

8. The apparatus of claim 1, wherein said control access to said data security device includes functionality for enabling or disabling ownership of said data security device, enabling or disabling enablement of said data security device, or enabling or disabling activation of said data security device.

9. A method for providing secure controllability of a data security device within a data processing system, said method comprising:

responsive to detecting a power-on reset cycle initiated within said data processing system:

determining the state of a pending state change flag, wherein said pending state change flag is write-accessible by runtime program instructions for setting an intended next state of a persistent enable flag that enables or disables runtime control access to said data security device, wherein said persistent enable flag is read-only accessible to runtime program instructions; and

setting or resetting said persistent enable flag in accordance with the state of said pending state change flag.

10. The method of claim 9, wherein said power-on reset steps are preceded by the step of setting said pending state change flag in accordance with user input during runtime operations of said data processing system.

11. The method of claim 9, further comprising, responsive to said pending state change flag being set, setting said persistent enable flag such that control access for said data security device is enabled following said power-on reset.

12. The method of claim 9, further comprising, responsive to said pending state change flag being reset, resetting said persistent enable flag such that control access for said data security device is disabled following said power-on reset.

13. (Cancelled)

14. The method of claim 9, wherein said power-on reset cycle includes execution of startup program instructions, said method further comprising:

responsive to receiving user input within said data processing system, setting or resetting a state of said pending state change flag in accordance with said user input; and

only in response to execution of said startup program instructions within said non-volatile programmable memory unit, updating said persistent enable flag to said intended state in accordance with the state of said pending state change flag.

15. The method of claim 9, wherein said data security device includes memory for receiving and storing data.

16. The method of claim 9, wherein said data security device includes security portal functionality for controlling access to data stored within said data processing system.

17. The method of claim 9, wherein said control access to said data security device includes functionality for enabling or disabling ownership of said data security device, enabling or disabling enablement of said data security device, or enabling or disabling activation of said data security device.

18. A computer-readable medium having encoded thereon computer-executable instructions for providing secure controllability of a data security device within a data processing system, said computer-executable instructions adapted for executing a method comprising:

program instructions responsive to detecting a power-on reset cycle initiated within said data processing system for:

determining the state of a pending state change flag, wherein said pending state change flag is write-accessible by runtime program instructions for setting an intended next state of a persistent enable flag that enables or disables runtime control access to said data security device, wherein said persistent enable flag is read-only accessible to runtime program instructions; and

setting or resetting said persistent enable flag in accordance with the state of said pending state change flag.

19. The computer-readable medium of claim 18, said method further comprising setting said pending state change flag in accordance with user input during runtime operations of said data processing system.

20. The computer-readable medium of claim 18, said method further comprising, responsive to said pending state change flag being set, setting said persistent enable flag such that control access for said data security device is enabled following said power-on reset.

21. The computer-readable medium of claim 18, said method further comprising, responsive to said pending state change flag being reset, resetting said persistent enable flag such that control access for said data security device is disabled following said power-on reset.

22. (Cancelled)

23. The computer-readable medium of claim 18, wherein said power-on reset cycle includes execution of startup program instructions, said method further comprising:

responsive to receiving user input within said data processing system, setting or resetting a state of said pending state change flag in accordance with said user input; and

responsive only to execution of said startup program instructions within said non-volatile programmable memory unit, updating said persistent enable flag to said intended state in accordance with the state of said pending state change flag.

24. The computer-readable medium of claim 18, wherein said data security device includes memory for receiving and storing data.

25. The computer-readable medium of claim 18, wherein said data security device includes security portal functionality for controlling access to data stored within said data processing system.

26. The computer-readable medium of claim 18, wherein said control access to said data security device includes functionality for enabling or disabling ownership of said data security device, enabling or disabling enablement of said data security device, or enabling or disabling activation of said data security device.

AMENDED CLAIMS APPENDIX

Claims as amended in After-Final Amendment filed concurrently herewith.

1. An apparatus for controlling access to a data security device within a data processing system, said apparatus comprising:

a persistent enable flag for providing control access to said data security device, wherein said persistent enable flag is write-accessible only in response to a detected power-on reset of said data processing system, and wherein said persistent enable flag is read-only accessible to runtime program instructions; and

a pending state change flag write-accessible by runtime program instructions, for setting an intended next state of said persistent enable flag such that control access to said data security device is enabled only during a subsequent power-on reset of said data processing system.

2. The apparatus of claim 1, further comprising:

a switched power input to said data security device;

a power-on reset detection latch for detecting the occurrence of power applied by said switched power input; and

means for determining the state of said power-on reset detection latch.

3. The apparatus of claim 2, further comprising means responsive to determining a set state of said power-on reset detection latch for:

determining the state of said pending state change flag; and

determining a next state of said persistent enable flag in accordance with the determined state of said pending state change flag.

4. (Cancelled)

5. The apparatus of claim 1, wherein said persistent enable flag and said pending state change flag are non-volatile storage devices.

6. The apparatus of claim 1, wherein said data security device includes memory for receiving and storing data.

7. The apparatus of claim 1, wherein said data security device includes security portal functionality for controlling access to data stored within said data processing system.

8. The apparatus of claim 1, wherein said control access to said data security device includes functionality for enabling or disabling ownership of said data security device, enabling or disabling enablement of said data security device, or enabling or disabling activation of said data security device.

9. A method for providing secure controllability of a data security device within a data processing system, said method comprising:

responsive to detecting a power-on reset cycle initiated within said data processing system:

determining the state of a pending state change flag, wherein said pending state change flag is write-accessible by runtime program instructions for setting an intended next state of a persistent enable flag that enables or disables runtime control access to said data security device, wherein said persistent enable flag is read-only accessible to runtime program instructions; and

setting or resetting said persistent enable flag in accordance with the state of said pending state change flag.

10. The method of claim 9, wherein said power-on reset steps are preceded by the step of setting said pending state change flag in accordance with user input during runtime operations of said data processing system.

11. The method of claim 9, further comprising, responsive to said pending state change flag being set, setting said persistent enable flag such that control access for said data security device is enabled following said power-on reset.

12. The method of claim 9, further comprising, responsive to said pending state change flag being reset, resetting said persistent enable flag such that control access for said data security device is disabled following said power-on reset.

13. (Cancelled)

14. The method of claim 9, wherein said power-on reset cycle includes execution of startup program instructions, said method further comprising:

responsive to receiving user input within said data processing system, setting or resetting a state of said pending state change flag in accordance with said user input; and

only in response to execution of said startup program instructions within said non-volatile programmable memory unit, updating said persistent enable flag to said intended state in accordance with the state of said pending state change flag.

15. The method of claim 9, wherein said data security device includes memory for receiving and storing data.

16. The method of claim 9, wherein said data security device includes security portal functionality for controlling access to data stored within said data processing system.

17. The method of claim 9, wherein said control access to said data security device includes functionality for enabling or disabling ownership of said data security device, enabling or disabling enablement of said data security device, or enabling or disabling activation of said data security device.

18. A computer-readable medium having encoded thereon computer-executable instructions for providing secure controllability of a data security device within a data processing system, said computer-executable instructions adapted for executing a method comprising:

responsive to detecting a power-on reset cycle initiated within said data processing system:

determining the state of a pending state change flag, wherein said pending state change flag is write-accessible by runtime program instructions for setting an intended next state of a persistent enable flag that enables or disables runtime control access to said data security device, wherein said persistent enable flag is read-only accessible to runtime program instructions; and

setting or resetting said persistent enable flag in accordance with the state of said pending state change flag.

19. The computer-readable medium of claim 18, said method further comprising setting said pending state change flag in accordance with user input during runtime operations of said data processing system.

20. The computer-readable medium of claim 18, said method further comprising, responsive to said pending state change flag being set, setting said persistent enable flag such that control access for said data security device is enabled following said power-on reset.

21. The computer-readable medium of claim 18, said method further comprising, responsive to said pending state change flag being reset, resetting said persistent enable flag such that control access for said data security device is disabled following said power-on reset.

22. (Cancelled)

23. The computer-readable medium of claim 18, wherein said power-on reset cycle includes execution of startup program instructions, said method further comprising:

responsive to receiving user input within said data processing system, setting or resetting a state of said pending state change flag in accordance with said user input; and

responsive only to execution of said startup program instructions within said non-volatile programmable memory unit, updating said persistent enable flag to said intended state in accordance with the state of said pending state change flag.

24. The computer-readable medium of claim 18, wherein said data security device includes memory for receiving and storing data.

25. The computer-readable medium of claim 18, wherein said data security device includes security portal functionality for controlling access to data stored within said data processing system.

26. The computer-readable medium of claim 18, wherein said control access to said data security device includes functionality for enabling or disabling ownership of said data security device, enabling or disabling enablement of said data security device, or enabling or disabling activation of said data security device.

EVIDENCE APPENDIX

Other than the Office Action(s) and reply(ies) already of record, no additional evidence has been entered by Appellants or the Examiner in the above-identified application which is relevant to this appeal.

RELATED PROCEEDINGS APPENDIX

There are no related proceedings as described by 37 C.F.R. §41.37(c)(1)(x) known to Appellants, Appellants' legal representative, or assignee.